ENGAGEMENT PERSONNEL

Je soussigné(e), ...déclare avoir pris connaissance du présent engagement de responsabilité et m'engage à en respecter le contenu et les règles de sécurité ci-dessous.

1. **Règles de sécurité et bonnes pratiques sur l'usage du système d'information**

   - L'utilisateur doit obligatoirement verrouiller son poste de travail lorsqu'il quitte son bureau (quelques secondes sont suffisantes à un utilisateur mal intentionné pour installer un programme malveillant sur un poste de travail);
   - L'utilisation de matériel personnel est interdite sur le système d'information de la DAP;
   - Le vol ou la perte d'un matériel informatique doit faire l'objet d'un rapport de vol qui doit être adressé au correspondant informatique et au responsable de la sécurité des systèmes d'information;
   - L'usage de matériel sans fil est interdit sur le système d'information (clef USB WiFi, clavier et souris sans fil...);
   - Les logiciels utilisés font obligatoirement l'objet d'une licence détenue par le bureau de des systèmes d'information de la DAP;
   - Les logiciels spécifiques doivent être installés par ce même bureau, l'installation de logiciel de jeux, de démonstration et de copie illicite sont interdites;
   - Afin d'éviter toutes propagations virales, il est de la responsabilité de l'utilisateur, en cas de détection d'un virus par l'antivirus, d'isoler son poste du travail du réseau (déconnexion du câble réseau sur la face arrière du poste) et de prévenir le support informatique et le responsable de la sécurité des systèmes d'information;
   - L'utilisateur est responsable des mots de passe qui lui permettent d'accéder au système d'information et aux applications présentes sur le système d'information. Ces mots de passe ne doivent jamais être divulgués, visibles ou facilement récupérables par autrui et doivent être changés tous les six mois. Ces mot de passe doivent contenir au moins 8 caractères minuscules ou majuscules et inclure des caractères spéciaux (#, !,@....) et des chiffres;
   - Les supports de stockage (disquette, cd-rom, clef USB) contenant des informations confidentielles doivent être enfermés au même titre que les documents papiers ;
   - Il est recommandé de sauvegarder les données professionnelles sur les lecteurs réseaux qui sont mis à disposition de l'utilisateur, afin d'en assurer leurs disponibilités (sauvegarde quotidienne automatique).
   - De façon plus générale, l'utilisateur doit signaler au service informatique référent toutes anomalies sur son poste de travail ;
   - Les ordinateurs portables doivent être équipés d'un câble antivol ou enfermés en lieu sûr lorsqu'ils ne sont pas utilisés ;